

the software constitutes acceptance of the terms on the user's part.

The most common type of license included with software purchased by individual users is a *single-user license agreement*, also called an *end-user license agreement (EULA)*. A single-user license agreement typically includes many of the following conditions that specify a user's responsibility upon acceptance of the agreement.

Users are permitted to:

- Install the software on only one computer. (Some license agreements allow users to install the software on one desktop computer and one notebook computer.)
- Make one copy of the software as a backup.
- Give or sell the software to another individual, but only if the software is removed from the user's computer first.

Users are not permitted to:

- Install the software on a network, such as a school computer lab.
- Give copies to friends and colleagues, while continuing to use the software.
- Export the software.
- Rent or lease the software.

Unless otherwise specified by a license agreement, you do not have the right to copy, loan, borrow, rent, or in any way distribute software. Doing so is a violation of copyright law. It also is a federal crime. Despite this, some experts estimate for every authorized copy of software in use, at least one unauthorized copy exists.

Software piracy continues for several reasons. In some countries, legal protection for software does not exist. In other countries, laws rarely are enforced. In addition, many buyers believe they have the right to copy the software for which they pay hundreds, even thousands, of dollars. Finally, software piracy is a fairly simple crime to commit.

Software piracy, however, is a serious offense. For one, it introduces a number of risks into the software market. It increases the chance of spreading viruses, reduces your ability to receive technical support, and drives up the price of software for all users. Further, software companies take illegal copying seriously. In some cases, offenders have been prosecuted to the fullest extent of the law with penalties including fines up to \$250,000 and five years in jail.

To promote a better understanding of software piracy problems and, if necessary, to take legal action, a number of major worldwide software companies formed the *Business Software Alliance (BSA)*. The BSA operates a Web site and antipiracy hotlines in the United States and more than 80 other countries.

In an attempt to prevent software piracy, Microsoft and other manufacturers have incorporated an activation process into many of their consumer products. During the **product activation**, which is conducted either online or by telephone, users provide the software product's 25-character identification number to receive an installation identification number unique to the computer on which the software is installed. Usually, the software does not function or has limited functionality until you activate it via the Internet or telephone.

Many organizations and businesses also have strict written policies governing the installation and use of software and enforce their rules by checking networked or online computers periodically to ensure that all software is licensed properly. If you are not completely familiar with your school or employer's policies governing installation of software, check with the information technology department or your school's technology coordinator.



WEB LINK 11-5

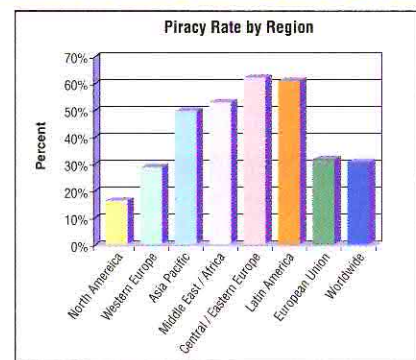
Business Software Alliance

For more information, visit scs.site.com/dc2009/ch11/weblink and then click Business Software Alliance.

FAQ 11-7

How prevalent is software piracy?

A recent study showed that approximately 35 percent of packaged software installed on personal computers worldwide was illegal. The chart to the right outlines some of the piracy rates around the world. For more information, visit scs.site.com/dc2009/ch11/faq and then click Software Piracy.



Source: Business Software Alliance

INFORMATION THEFT

Information theft is yet another type of computer security risk. **Information theft** occurs when someone steals personal or confidential information. If stolen, the loss of information can cause as much damage as (if not more than) hardware or software theft.

Both business and home users can fall victim to information theft. An unethical company executive may steal or buy stolen information to learn about a competitor. A corrupt individual may steal credit card numbers to make fraudulent purchases. Information theft often is linked to other types of computer crime. For example, an individual first might gain unauthorized access to a computer and then steal credit card numbers stored in a firm's accounting department.

Information transmitted over networks offers a higher degree of risk because unscrupulous users can intercept it during transmission. Every computer along the path of your data can see what you send and receive. Ironically, though, studies show that the biggest threat to a business' information is its internal employees.

Safeguards against Information Theft

Most companies will attempt to prevent information theft by implementing the user identification and authentication controls discussed earlier in this chapter. These controls are best suited for protecting information on computers located on a company's premises.

To protect information on the Internet and networks, companies and individuals use a variety of encryption techniques to keep data secure and private.

Encryption

Encryption is a process of converting readable data into unreadable characters to prevent unauthorized access. You treat encrypted data just like any other data. That is, you can store it or send it in an e-mail message. To read the data, the recipient must **decrypt**, or decipher, it into a readable form.

In the encryption process, the unencrypted, readable data is called *plaintext*. The encrypted

(scrambled) data is called *ciphertext*. To encrypt the data, the originator of the data converts the plaintext into ciphertext using an encryption key. In its simplest form, an *encryption key* is a programmed formula that the recipient of the data uses to decrypt ciphertext. For a more technical discussion about encryption keys, read the High-Tech Talk article on page 592.

Many data encryption methods exist. Figure 11-16 shows examples of some simple encryption methods. An encryption key (formula) often uses more than one of these methods, such as a combination of transposition and substitution. Most organizations use available software for encryption. Others develop their own encryption programs. With Windows Vista's *Encrypting File System*, you easily can encrypt the contents of files and folders. To display the Windows Vista dialog box shown in Figure 11-17, right-click the file or folder name in Explorer, click Properties on the shortcut menu, click the General tab, and then click the Advanced button in the Properties dialog box. Windows Vista also includes a feature called *BitLocker* that allows you to encrypt all files on a drive.

When users send an e-mail message over the Internet, they never know who might intercept it, who might read it, or to whom it might be forwarded. If a message contains personal or confidential information, users can protect the message by encrypting it or signing it digitally. Some e-mail programs allow you to encrypt the messages that are stored on your computer. To decrypt the messages, you use a password separate from the one you use to access your e-mail account. One of the more popular e-mail encryption programs is called *Pretty Good Privacy* (PGP). PGP is freeware for personal, noncommercial users. Home users can download PGP from the Web at no cost.

SAMPLE ENCRYPTION METHODS

Name	Method	Plaintext	Ciphertext	Explanation
Transposition	Switch the order of characters	SOFTWARE	OSTFAWER	Adjacent characters swapped
Substitution	Replace characters with other characters	INFORMATION	WLDIMXQUWIL	Each letter replaced with another
Expansion	Insert characters between existing characters	USER	UYSYERY	Letter Y inserted after each character
Compaction	Remove characters and store elsewhere	ACTIVATION	ACIVTIN	Every third letter removed (T, A, O)

FIGURE 11-16 This table shows four simple methods of encryption. Most encryption programs use a combination of these four methods.

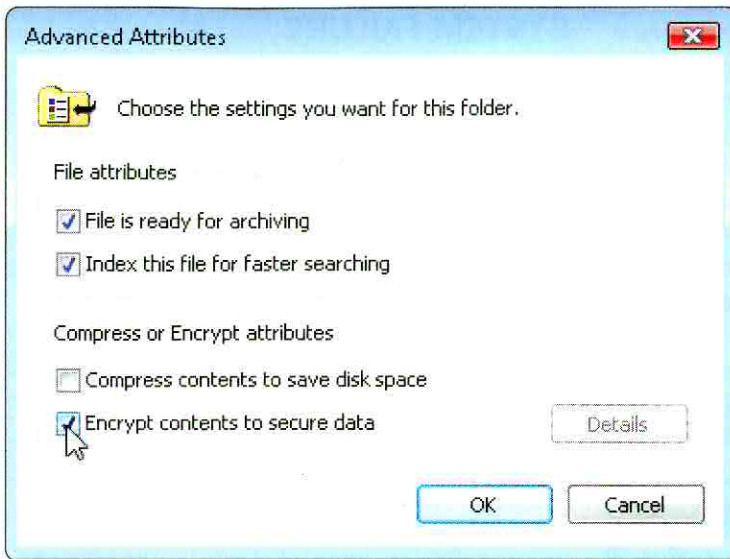


FIGURE 11-17 Through this Windows Vista dialog box, you can encrypt files and folders. Only the user that encrypted the files and folders can access them.

WEB LINK 11-6

BitLocker

For more information, visit scs.site.com/dc2009/ch11/weblink and then click BitLocker.

A **digital signature** is an encrypted code that a person, Web site, or company attaches to an electronic message to verify the identity of the message sender. The code usually consists of the user's name and a hash of all or part of the message. A *hash* is a mathematical formula that generates a code from the contents of the message. Thus, the hash differs for each message. Receivers of the message decrypt the digital signature. The recipient generates a new hash of the received message and compares it with one in the digital signature to ensure they match.

Digital signatures often are used to ensure that an impostor is not participating in an Internet transaction. That is, digital signatures help to prevent e-mail forgery. A digital signature also can verify that the content of a message has not changed.

Many Web browsers also use encryption. Some browsers offer a protection level known as *40-bit encryption*. Many also offer *128-bit encryption* and *1024-bit encryption*, which are even higher levels of protection because they have longer encryption keys. Applications requiring more security, such as banks, brokerage firms, or online retailers that use credit card or other financial information, require 128-bit or 1024-bit encryption.

A Web site that uses encryption techniques to secure its data is known as a **secure site**. Secure sites use digital certificates along with a security protocol. Two popular security protocols are Secure Sockets Layer and Secure HTTP. Organizations often use VPNs. The following paragraphs briefly discuss security techniques.

DIGITAL CERTIFICATES A digital certificate is a notice that guarantees a user or a Web site is

legitimate. E-commerce applications commonly use digital certificates. Web browsers, such as Internet Explorer, often display a warning message if a Web site does not have a valid digital certificate.

A **certificate authority (CA)** is an authorized person or a company that issues and verifies digital certificates. Users apply for a digital certificate from a CA (Figure 11-18). A digital certificate typically contains information such as the user's name, the issuing CA's name and signature, and the serial number of the certificate. The information in a digital certificate is encrypted.

WEB LINK 11-7

Digital Certificates

For more information, visit scs.site.com/dc2009/ch11/weblink and then click Digital Certificates.



FIGURE 11-18 A certificate authority issues and verifies digital certificates.

SECURE SOCKETS LAYER *Secure Sockets Layer* (SSL) provides encryption of all data that passes between a client and an Internet server. SSL requires the client have a digital certificate. Once the server has a digital certificate, the Web browser communicates securely with the client. Web addresses of pages that use SSL typically begin with https, instead of http (Figure 11-19). SSL is available in 128-bit encryption and higher.

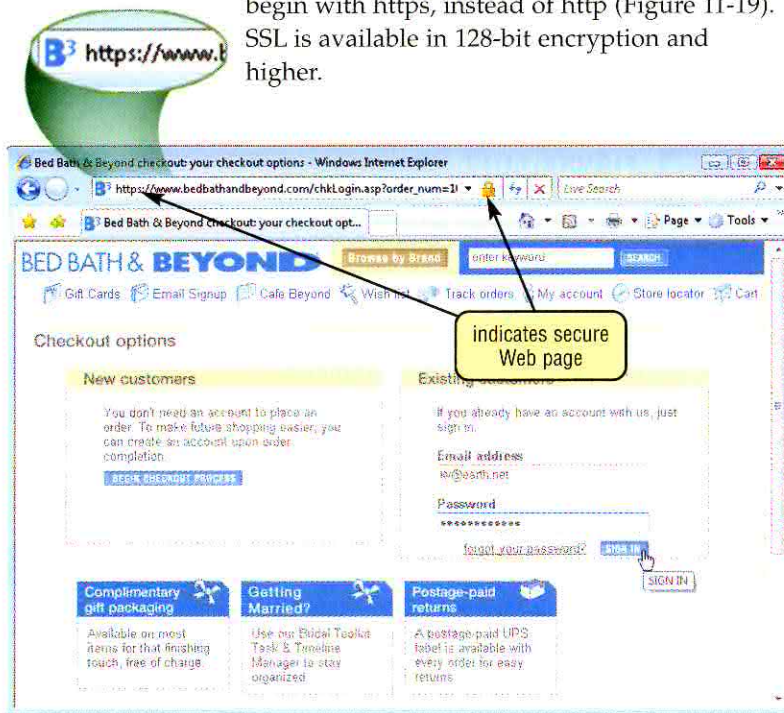


FIGURE 11-19 Web addresses of secure sites often begin with https instead of http. Secure sites also often display a lock symbol in the window.

SECURE HTTP *Secure HTTP (S-HTTP)* allows users to choose an encryption scheme for data that passes between a client and a server. With S-HTTP, the client and server both must have digital certificates. S-HTTP is more difficult to use than SSL, but it is more secure. Applications that must verify the authenticity of a client, such as for online banking, use S-HTTP.

VPN Mobile users today often access their company networks through a virtual private network. When a mobile user connects to a main office using a standard Internet connection, a *virtual private network (VPN)* provides the mobile user with a secure connection to the company network server, as if the user has a private line. VPNs help ensure that data is safe from being intercepted by unauthorized people by encrypting data as it transmits from a notebook computer, Tablet PC, smart phone, PDA, or other mobile device.

SYSTEM FAILURE

System failure is yet another type of computer security risk. A *system failure* is the prolonged malfunction of a computer. System failure also can cause loss of hardware, software, data, or information. A variety of causes can lead to system failure. These include aging hardware; natural disasters such as fires, floods, or hurricanes; random events such as electrical power problems; and even errors in computer programs.

One of the more common causes of system failure is an electrical power variation. Electrical power variations can cause loss of data and loss of equipment. If the computer equipment is networked, a single power disturbance can damage multiple systems. Electrical disturbances include noise, undervoltages, and overvoltages.

Noise is any unwanted signal, usually varying quickly, that is mixed with the normal voltage entering the computer. Noise is caused by external devices such as fluorescent lighting, radios, and televisions, as well as by components within the computer itself. Noise generally is not a risk to hardware, software, or data. Computer power supplies, however, do filter out noise.

An **undervoltage** occurs when the electrical supply drops. In North America, a wall plug usually supplies electricity at approximately 120 volts. Any significant drop below 120 volts is an undervoltage. A *brownout* is a prolonged undervoltage. A *blackout* is a complete power failure. Undervoltages can cause data loss but generally do not cause equipment damage.

An **overvoltage**, or **power surge**, occurs when the incoming electrical power increases significantly above the normal 120 volts. A momentary overvoltage, which is called a *spike*, occurs when the increase in power lasts for less than one millisecond (one thousandth of a second). Uncontrollable disturbances such as lightning bolts can cause spikes. Overvoltages can cause immediate and permanent damage to hardware.

Safeguards against System Failure

To protect against electrical power variations, use a surge protector. A **surge protector**, also called a *surge suppressor*, uses special electrical components to smooth out minor noise, provide a stable current flow, and keep an overvoltage from reaching the computer and other electronic equipment (Figure 11-20). Sometimes resembling a power strip, the computer and other devices plug in the surge protector, which plugs in the